Asci, Terry (SCA)

From: noreply@formstack.com
Sent: Wednesday, January 23, 2019 10:36 AM
To: Breaches, Data (SCA)
Subject: Security Breach Notifications

Formstack Submission For: Security Breach Notifications - With Addresses

Submitted at 01/23/19 10:35 AM

Business Name:	ALM Media, LLC
Is the business located in the United States?:	Yes
Business Address:	150 East 42nd Street New York, NY 10017
Foreign Business Address:	
Company Type:	Commercial
Your Name:	Jason Wool
Title:	Counsel
Contact Address:	ZwillGen PLLC 1900 M Street NW, Suite 250 Washington, DC 20036
Contact Address:	
Telephone Number:	(202) 706-5216
Extension:	

Email Address:	jason@zwillgen.com
Relationship to Org:	Third party provider
Breach Type:	Electronic
Date Breach was Discovered:	12/28/2018
Number of Massachusetts Residents Affected:	30
Person responsible for data breach.:	Unknown
Please give a detailed explanation of how the data breach occurred.:	In late December, ALM learned that an unknown third party had uploaded JavaScript code to several e-commerce pages used to process payments for various products. ALM quickly commenced an investigation to understand the code' s functionality and engaged third-party cybersecurity experts to assist with this analysis. ALM also disabled the checkout feature of the affected sites while it worked to remove the unauthorized code and instead directed customers to purchase products by phone. On December 28, 2018, ALM determined that the code was designed to collect and transmit to an unknown third party the payment card details of customers making purchases on the affected sites. ALM determined that the unauthorized code was present on the affected websites from July 7, 2018 until December 24, 2018.
Please select the type of personal information that was included in the breached data.:	Credit/Debit Card Number = Selection(s)
Please check ALL of the boxes that apply to your breach.:	The breach was a result of a malicious/criminal act. = Selection(s)
For breaches involving paper: A lock or security mechanism was used to physically protect the data.:	N/A
Physical access to systems containing personal information was restricted to authorized personnel only.:	Yes

Network configuration of breached system:	Internet Access Available
For breaches involving electronic systems, complete the following:	N/A = Selection(s)
Does your business maintain a Written Information Security Program (WISP)?:	Yes
All Massachusetts residents affected by the breach have been notified of the breach.:	Yes
Method(s) used to notify Massachusetts residents affected by the breach (check all that apply)::	Option2 | US Mail
Please explain your answer of Other Above:	
Date notices were first sent to Massachusetts residents (MM/DD/YYYY):	01/23/2019
All Massachusetts residents affected by the breach have been offered complimentary credit monitoring services.:	Yes
Law enforcement has been notified of this data breach.:	No
Please describe how your company responded to the breach. Include what changes were made or may be made to prevent another similar breach from occurring, including updating your WISP.:	In addition to the measures described above, ALM is using a third party web application security scanning tool, which would alert the company to any security vulnerabilities or other externally visible issues that could affect the security of the e-commerce pages. In addition, the company is using an internal security monitoring tool on the e-commerce platform, which provides daily reports on security configurations, the presence of new files, and changes to existing files on the website's file system.
Yes / No:	Yes

File 1 Upload:	View File
File 2 Upload:	
File 3 Upload:	
File - 4 Upload:	

Formstack, 8604 Allisonville Road, Suite 300, Indianapolis, IN 46250

1436

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Notice of Data Breach

Dear <<Name 1>>:

We are writing to notify you of an incident that may have affected the confidentiality of your personal information. In particular, we recently learned that some of our e-commerce websites were subject to a sophisticated cyber-attack apparently targeting the payment card information of some of our customers, including yours.

ALM greatly values our customers, and we take the security of your personal information very seriously. We regret this situation and any inconvenience or concern it may cause you. We have set forth below information about the steps you can take to protect yourself following this incident. Please review this information carefully.

What Happened?

In late December 2018, ALM learned that an unknown third party had obtained unauthorized access to several websites used to process payments for various products sold under The National Underwriter and Judy Diamond brands. ALM quickly commenced an investigation to understand the nature of the compromise and engaged third-party cybersecurity experts to assist with this analysis. We also promptly disabled the checkout page on the affected sites pending the results of our investigation. On December 28, 2018, ALM determined that the compromise was designed to collect and transmit to an unknown third party the payment card details of customers making purchases on the affected sites. ALM determined that the compromise of the affected websites lasted from July 7, 2018 until December 24, 2018.

What Information Was Involved?

The data elements acquired in connection with the compromise included a customer's name, billing/shipping address, telephone and fax number, payment card account number, payment card expiration date, and the payment card verification number (i.e., the number printed on the front or back of your payment card used in online transactions to verify that you possess the card).

What We Are Doing.

We have removed the compromised portion of the sites in question and taken steps in response to this incident to better withstand these types of cyber-attacks on our e-commerce platform in the future. In addition, to help protect your identity, we are offering one complimentary year of enrollment in TransUnion's *my*TrueIdentity Credit Monitoring Service. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. Details on how to enroll in the TransUnion credit monitoring service and additional detail on the service's features are provided below.

What You Can Do.

In addition to enrolling in the TransUnion credit monitoring service, we recommend that you remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports for any unauthorized activity. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported. There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please see the attachment to this letter.

For More Information.

We sincerely regret any inconvenience this incident may cause you, and we encourage you to take advantage of the TransUnion credit monitoring service being offered. Should you have questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact us at **877-291-9451**.

Sincerely,

William Carter
Chief Executive Officer
ALM Media, LLC

SUPPLEMENTAL INFORMATION

It is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-685-1111	1-888-397-3742	1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

If you are a resident of California, Connecticut, Iowa, Maryland, Massachusetts, North Carolina, Oregon, or Rhode Island, you may contact and obtain information from and/or report identity theft to your state attorney general at:

California Attorney General's Office, California Department of Justice, Attn: Office of Privacy Protection, P.O. Box 944255, Sacramento, CA 94244-2550, (800) 952-5225, https:oag.ca.gov/

Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, (515) 281-5164, www.iowaattorneygeneral.gov

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023 or 1-410-576-6300

Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400 or 1-877-566-7226

Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (503) 378-4400, http://www.doj.state.or.us/

Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

If you are a resident of Massachusetts or Rhode Island, note that pursuant to Massachusetts or Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze.

If you are a resident of West Virginia, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

Experian Security Freeze	**TransUnion Security Freeze**	**Equifax Security Freeze**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
www.experian.com	www.transunion.com	www.equifax.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

In Addition, New Mexico Consumers Have the Right to Submit a Declaration of Removal. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft.

TransUnion

Activation Code:
<<Activation Code>>

Complimentary One-Year *my*TrueIdentity Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)